

**TITLE**

**Accelerated Test Method and System**

**BACKGROUND**

**Field of Invention**

5       The present invention relates to an accelerated test method and system. More particularly, the present invention relates to an accelerated test method and system using a one-way-hash function to reduce the integrated circuit test time.

10      **Description of Related Art**

In the integrated circuit industry, test time is a substantial expense factor in the total cost of device production, especially for the latest multi-million gate designs. In some cases, the cost of the test is higher than the manufacturing cost. Shortening the test time will reduce the production cost.

15       Fig. 1 shows a traditional verification method used in an integrated circuit test. The traditional verification method relies on data analysis of the test, recorded and analyzed sequentially. For example, a large amount of test vector data 102 is sent to the integrated circuit 104 and the response data 106 is produced in response to the test vector data 102. The response data 106 is  
20      recorded and analyzed in the automated test equipment (ATE) 108. A database 110 that stores standard response data is used in the verification process in the automated test equipment 108. Since there is a lot of response data 106 to be verified, the test process consumes a large amount of automated test equipment resource as well as test time.

## SUMMARY

The present invention is directed to an accelerated test method and system that satisfy the need to reduce the integrated circuit test time as well as  
5 save the production cost.

It is therefore an objective of the present invention to provide an accelerated test method for testing an integrated circuit. It is a method to reduce the integrated circuit test time as well as the production cost.

It is another objective of the present invention to provide an accelerated  
10 test method for testing an integrated circuit. The accelerated test method greatly reduces the memory used in the automated test equipment during test.

It is still another objective of the present invention to provide an accelerated test method for testing an integrated circuit. With a one-way-hash module imbedded in the BIST of the integrated circuit under test, the test  
15 process is accelerated when the IO speed is the bottleneck of the test process.

In accordance with the foregoing and other objectives of the present invention, an accelerated test method for testing an integrated circuit is disclosed. The accelerated test method includes the following steps. First, test vector data is taken as input for the integrated circuit to produce response  
20 data as output. Next, a one-way-hash function is used to transform the response data into a test message digest. Next, the test message digest is verified against a standard message digest to determine whether the test message digest meet a predetermined requirement.

The one-way-hash function is, for example, a SHA-1 or a MD5. The  
25 one-way-hash function is performed by a one-way-hash hardware circuit. A

SHAX, for example, is a hardware circuit that performs SHA-1. The one-way-hash hardware circuit is embedded as part of the BIST circuit in the integrated circuit.

The one-way-hash function is also suitable for implementation in  
5 automated test equipment. For example, the one-way-hash function is performed by a specifically designed single chip in the automated test equipment. A microprocessor or a DSP can be used to perform the one-way-hash function in the automated test equipment.

Because the response data is largely reduced by the one-way-hash  
10 module, the integrated circuit test time and the production cost are also reduced.

Only the test message digest is verified in the automated test equipment, so the memory used in the automated test equipment is reduced. With a one-way-hash module imbedded in the BIST of the integrated circuit under test,  
15 the test message digest is generated before being sent to the automated test equipment via the IO interface. Therefore, the test process is accelerated when the IO speed is the bottleneck of the test process.

It is to be understood that both the foregoing general description and the following detailed description are by examples, and are intended to provide further explanation of the invention as claimed.

20

#### BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of  
25 this specification. The drawings illustrate embodiments of the invention and,

together with the description, serve to explain the principles of the invention. In the drawings,

Fig. 1 is a diagram of the prior art;

Fig. 2A is a diagram of the accelerated test method of the invention;

5 Fig. 2B is a flow chart illustrating the accelerated test method of the invention;

Fig. 3 is a block diagram illustrating the first preferred embodiment of the invention;

10 Fig. 4 is a block diagram illustrating the second preferred embodiment of the invention; and

Fig. 5 is a block diagram illustrating the third preferred embodiment of the invention.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

15

Reference will now be made in detail to the present preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the description to refer to the same or like parts.

20 The accelerated test method is used for testing an integrated circuit.

Fig. 2A is a diagram of the accelerated test method of the invention. Fig. 2B is a flow chart illustrating the accelerated test method of the invention.

First, test vector data 202 is taken as input to an integrated circuit 204 to produce response data 206 as output (step 220 and step 222). The response 25 data 206 is then sent to a one-way-hash module 208 that performs a

one-way-hash function. The one-way-hash function is, for example, a SHA-1 or a MD5. An example of the one-way-hash module 208 is a SHAX that performs SHA-1.

Next, the one-way-hash module 208 is used to transform the response data 206 into a test message digest 210 (step 224). Next, the test message digest 210 is verified against a standard message digest (step 226). For example, the verification process is performed by comparing the test message digest 210 with the standard message digest 212 to determine whether the test message digest 210 meets a predetermined requirement.

ATM is the acronym for “accelerated test method”. As mentioned above, ATM uses a one-way-hash function to condense the response data 206 of the integrated circuit under test (after responding to the test vector data 202) into the test message digest 210. The test message digest 210 is equivalent to a unique signature of the integrated circuit 204. The test message digest 210 is verified against the golden signature that is known to be absolutely correct and true. The golden signature is the standard message digest 212 shown in Fig. 2A.

The standard message digest 212 is obtained by the following exemplary method. First, a standard integrated circuit, which has been verified, is selected. Next, the test vector data 202 is taken as input to the standard integrated circuit and a standard response data is produced as output. Next, the one-way-hash module 208 is used to transform the standard response data into the standard message digest 212.

Another example of obtaining the standard message digest 212 is to simulate the behavior of the integrated circuit as well as the one-way-hash

function in a computer and to generate the standard message digest in response to the test vector data.

With ATM there is no large amount of data to verify. Only the test message digest 210 of the test response data 206 is verified. The test 5 message digest 210 is extremely short compared to the response data 206. For example, SHAX produces a 160-bit test message digest. Verification of such a short test message digest is very quick and virtually without cost regarding processor resources. For example, hardware XOR of the test message digest 210 and the standard message digest 212 is an efficient 10 implementation for verification.

ATM can be applied to both Scan Testing and BIST methodologies. Fig. 3 shows a first preferred embodiment of the invention. The integrated circuit 308 has a main module 314 and a BIST circuit 306. The main module 314 is used to perform the main function of the integrated circuit 308. The one-way-hash function is performed by a one-way-hash module 302. The one-way-hash module 302 is a hardware circuit and embedded as part of the BIST circuit 306 in the integrated circuit 308. BIST stands for 15 Built-In-Self-Test.

The automated test equipment 304 sends test vector data 310 to the 20 integrated circuit 308. The one-way-hash-module 302 performs the one-way-hash function on the test response data to generate a test message digest 312. The automated test equipment 304 receives the test message digest 312 and verifies it against the standard message digest.

Fig. 4 shows a second preferred embodiment of the invention. The 25 integrated circuit 402 includes a plurality of IP (intellectual property) blocks and

a plurality of one-way-hash modules are respectively embedded in corresponding IP blocks as part of the BIST circuit in said IP blocks.

For example, the integrated circuit 402 has three IP blocks (IP1 410, IP2 412, and IP3 414). One-way-hash modules 404, 406, and 408 are embedded 5 in IP1 410, IP2 412, and IP3 414, respectively. One-way-hash modules 404, 406, and 408 are all hardware circuits and serve as part of the BIST circuit of IP1 410, IP2 412, and IP3 414, respectively.

As shown in Fig. 4, the automated test equipment 416 – that supports CCT technology – sends test vector data 418, 420, and 422 to IP1 410, IP2 412, 10 and IP3 414 respectively. The test message digest 424, 426, and 428 are generated by one-way-hash modules 404, 406, and 408, respectively, and then sent to the automated test equipment 416. The test message digest 424, 426, and 428 are verified in the automated test equipment 416.

Fig. 5 shows a third preferred embodiment according to the invention. 15 The one-way-hash function is performed by a one-way-hash module 502. The one-way-hash module 502 is a hardware circuit and implemented within automated test equipment 504. The automated test equipment 504 sends a test vector data 506 to an integrated circuit 508 and receives response data 510 from the integrated circuit 508. The one-way-hash module 502 receives 20 response data 510 to generate a test message digest to be verified in the automated test equipment 504. The response data 510 is processed on-the-fly by the automated test equipment 504 and no memory is required to store the response data 510. When all test vector data 506 is driven, the test message digest is ready for verification as well. The automated test equipment 504

verifies the test message digest against the standard message digest and no memory is required to store the standard response data.

For example, a chip is specifically designed for performing the one-way-hash function and implemented within the automated test equipment

5 504. In another example, the one-way-hash function is performed by a microprocessor or a DSP in the automated test equipment 504.

When integrated into the automated test equipment 504, the one-way-hash module 502 helps to reduce the memory and data processing time. The automated test equipment 504 no longer needs to store large

10 amount of test response data 510 or standard response data and perform analysis.

SHAX is a highly suitable hardware for the one-way-hash module in any of the three preferred embodiments mentioned above. SHAX stands for Secure Hash Algorithm Accelerator. SHAX is an embedded hardware

15 accelerator that performs SHA-1 on a message. Performing SHA-1 on a 512-bit message block by software would normally require more than 10,000 instructions and at least as many clock cycles to complete the task. SHAX

needs less than 100 clock cycles to complete the same task. SHAX produces a 160 bits message digest for any message less than  $2^{64}$  bits in length, which is

20 plenty for any device test.

SHAX completes SHA-1 in just 81 clocks. The maximum number of clocks required to completely process a 512-bit message block is 99 clocks. That includes 1 clock for the optional configuration, 16 clocks to load the message, 1 clock to start SHA-1, and 81 clocks to complete SHA-1.

For example, the SHAX is designed with Verilog RTL and is 100% technology independent. Thus, it is always ready to be embedded in an integrated circuit. The FPGA implementation on Virtex 300E is estimated as 26,000 equivalent gate count reported by Xilinx ISE 5.1. The logic gate count 5 of ASIC implementation is estimated in the range between 15,000 and 20,000.

Although the present invention has been described in considerable detail with reference to certain preferred embodiments thereof, other embodiments are possible. Therefore, their spirit and scope of the appended claims should not be limited to the description of the preferred embodiments contained herein.

10 It will be apparent to those skilled in the art that various modifications and variations can be made to the structure of the present invention without departing from the scope or spirit of the invention. In view of the foregoing, it is intended that the present invention cover modifications and variations of this invention provided they fall within the scope of the following claims and their 15 equivalents.